



# UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,621	06/25/2003	Shigeto Hiraga	500.42888X00	2511

24956 7590 09/23/2005

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.  
1800 DIAGONAL ROAD  
SUITE 370  
ALEXANDRIA, VA 22314

EXAMINER

HICKS, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2165

DATE MAILED: 09/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

10/602,621

Applicant(s)

HIRAGA ET AL.

Examiner

Michael J. Hicks

Art Unit

2165

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 06/25/2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-11 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-11 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 25 June 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 9/17/03; 3/21/05
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Drawings***

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 100, 110, 120, 130, 140, 150, 160, 170, 303, and 605. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

### ***Specification***

2. The disclosure is objected to because of the following informalities: On page 12, Lines 12-22, in regards to step 606 of Figure 6, two distinctly different outcomes, one leading to step 607 and the other leading to step 608, are given for if the result of the step is yes, while none are given for if the outcome of the step is no. Furthermore, it is

Art Unit: 2165

clearly illustrated in Figure 6, that one outcome should produce a result of yes, and lead to step 607, while the other should produce a result of no, and lead to step 608. This creates an inconsistency between the specification and the drawings which requires appropriate correction.

***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 7 rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

According to the Prior Art of Record, a database manager, or database administrator is one who has the authorization to assign access controls and is not constrained by any themselves. According to Claim 7, the privileges of the database manager are also constrained by access controls, which would restrict their ability to assign and manage access controls to other users as well as their ability to manage data in the system. Applicant does not disclose, nor would it be obvious to one skilled

Art Unit: 2165

in the art, how to manage the access rights of the database manager if their ability to manage these access rights is constrained by access controls.

6. Claims 2, 4, and 6 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per Claim 2, in lines 6-7 of Claim 2, in the phrase "while if not, the deletion of said to be deleted is prohibited" does not specify what is to be deleted, therefor rendering the claim vague and indefinite.

For the purpose of further consideration, it will be assumed that what is to be deleted is data.

As per Claim 4, the limitation "said deletion prohibition period" is recited in lines 4-5. There is insufficient antecedent basis for this limitation in the claim.

As per Claim 6, the limitation "said database to be unloaded" is recited in line 3. There is insufficient antecedent basis for this limitation in the claim.

### ***Claim Rejections - 35 USC § 102***

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-4, and 6-11 rejected under 35 U.S.C. 102(b) as being anticipated by Glover et al. ("Multilevel Secure Databases: A New Approach", IEEE Proceedings of

Southeastcon '91, Apr. 1991; Vol. 2, Pgs 690-694, and referred to hereinafter as Glover).

As per Claims 1 and 9, Glover discloses a database management method and program, comprising the steps of: entering a database definition request including identification information for specifying a database and access attribute information of said database (i.e. *"The data dictionary contains the database schema and characteristics of data attributes. The data dictionary is invoked for data validation whenever a query is posed or data is updated or added to the database...The data dictionary may also contain information about discretionary access privileges and the location of database files which contain the actual data."* The preceding text excerpt clearly indicates that whenever a query/update/data addition is requested the data dictionary is invoked and provides information about/defines the database (in affect making the query/update/data addition a data definition request), such information including the database schema/characteristics of data attributes/identification information for specifying a database and information about discretionary access privileges/access attribute information of said database.) (Page 692, Under Heading: **Secure Data Dictionary**); if said access attribute information is an insert-only attribute, authorizing data insertion and access to data in said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified with only the insert privilege/is an insert-only attribute, then only access to the data and data insertion will be allowed/authorized.) (Page 691, Under Heading: **Discretionary Access Control**); specifying at least an attribute of data update prohibition to

said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified as not including the update right/specifying an attribute of data update prohibition, the user will not be able to update database information.) (Page 691, Under Heading: **Discretionary Access Control**); and disabling change of said attribute after said attribute is specified (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists."* The preceding text excerpt clearly indicates that another user is not able to grant any privileges to a user not granted by the DBA, nor is the user able to change the level of their access rights (i.e. change of said attribute is disabled).) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 2, Glover discloses said access attribute information including a deletion prohibition period, and if said deletion prohibition period has passed since the time when said data to be deleted was registered, deletion of said data to be deleted is authorized, while if not, the deletion of said to be deleted is prohibited (i.e. *" In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing....Access control rules are written by the DBA using QUEL. Integrity constraints are expressed in QUEL by the DEFINE PERMIT statement as follows: DEFINE PERMIT <operations> on <relation> [(field-comma list)] to user [at terminal] [from time1 to time2] [on day1 to day2] [where*

Art Unit: 2165

*condition]*" The preceding text excerpt clearly indicates that a deletion prohibition period could be created if a DEFINE PERMIT operation were executed on a newly inserted item of data, specifying a later time at which the data could be updated. Specifically, if a DEFINE PERMIT operation were executed on a newly inserted piece of data where the *<operation>* field indicated the operation of deleting data, and the *[from time1 to time2]* field specified a time frame which began later than the current/registration time, or the *[on day1 to day2]* specified a range of days which began after the current day. The data prohibition period would then be the period of time from the current time (i.e. the time of creation/registration) up to the beginning of the timeframe specified in the *[from time1 to time2]*, or the *[on day1 to day2]* fields. Note that until the beginning of this timeframe/during the deletion prohibition period, the delete operation would not be allowed/deletion of said data to be deleted would be prohibited, but after the start of the timeframe/after the deletion prohibition period the operation of data deletion would be allowed/deletion of said data to be deleted is authorized. Alternately, the *[where condition]* field could be used in place of the *[from time1 to time2]* or *[on day1 to day2]* fields by specifying that data deletion is to be permitted only if the current system timestamp is greater than a timestamp created upon the insertion/registration of the data plus a set amount of time which would be considered the deletion prohibition period. Note that timestamping and the operation of performing addition and comparison on times and dates is supported in query languages and would have been known to one skilled in the art at the time of Applicant's invention.) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 3, Glover discloses data deletion prohibition being specified to said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."*) The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified as not



including the delete right/specifying data deletion prohibition, the user will not be able to delete database information.) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 4, Glover discloses any one of change of a database name, deletion of a database, release of said insert-only attribute, and change of said deletion prohibition period is prohibited in said database (i.e. "*In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update.*" The preceding text excerpt clearly indicates that another user is not able to grant any privileges to a user not granted by the DBA, nor is the user able to change the level of their access rights, including the insert only attribute (i.e. release of said insert-only, or deletion prohibition attributes is prohibited).) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 6, Glover discloses that if no insert-only attribute is specified to said database to be unloaded, the reload of said database with said insert-only attribute specified thereto is prohibited (i.e. "*In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update.*" The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified with only the insert privilege/is an insert-only attribute, then only access to the data and data insertion will be allowed/authorized. Note that because a restore/reload of a database will include either

the deletion or the update of data in the database, the reload operations would not be permitted due to the fact that only data access and data insertion is permitted as previously stated.) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 7, Glover discloses an access control for said database being applied to access of all users including a database manager (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorizations...Mandatory security refers to the enforcement of a set of access control rules that constrain a subject's access to information on the basis of a comparison of the individual's clearance, the classification of the information, and the form of access being mediated."* The preceding text excerpt clearly indicates all users are constrained by Mandatory security (therefor access control is applied to all users) and also, because the DBA/database manager is responsible for all authorizations, it would be possible for the DBA/database manager to apply authorization rules to themselves.) (Page 691, Under Heading: **Discretionary Access Control**; Pages 690-691, Under Heading: **System Security Policy**).

As per Claim 8, Glover discloses a database management apparatus comprising: means for entering a database definition request including specifying a database and access attribute information of said database (i.e. *"The data dictionary contains the database schema and characteristics of data attributes. The data dictionary is invoked for data validation whenever a query is posed or data is updated or added to the database...The data dictionary may also contain information about discretionary access privileges and the location of database files which contain the actual data."* The preceding text excerpt clearly indicates that whenever a query/update/data addition is requested the data dictionary is invoked and provides information about/defines the database (in affect making the query/update/data addition a data definition request), such information including the database schema/characteristics of data attributes/identification information for specifying a database and information about discretionary access privileges/access attribute information of said database.) (Page 692, Under Heading: **Secure Data Dictionary**); and means for, if said database definition

request is a first specification of an insert-only attribute, authorizing data insertion and data access in said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified with only the insert privilege/is an insert-only attribute, then only access to the data and data insertion will be allowed/authorized. Note that the rights of data access and data insertion will be granted on the first specification of the access rights/attributes as well as all subsequent specifications.) (Page 691, Under Heading: **Discretionary Access Control**) and specifying least a data update prohibition attribute to said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified with only the insert privilege/is an insert-only attribute, then only access to the data and data insertion will be allowed/authorized.) (Page 691, Under Heading: **Discretionary Access Control**).

As per Claim 10, Glover discloses said access attribute information including a data update postponement period, if said data update postponement period has not passed since the time when said data with said postponement period specified thereto

was inserted, the update of said data is authorized, and if said postponement period has passed, said data update is prohibited (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing...Access control rules are written by the DBA using QUEL. Integrity constraints are expressed in QUEL by the DEFINE PERMIT statement as follows: DEFINE PERMIT <operations> on <relation> [(field-comma list)] to user [at terminal] [from time1 to time2] [on day1 to day2] [where condition]"*) The preceding text excerpt clearly indicates that the access rules/attribute information can include a data update postponement period. Specifically, the DBA can allow a user (or all users, specified in the *user* field) to update (specified in the *<operations>* field) any of the relations/data specified in the *<relation> [(field-comma list)]* field during the time period specified in the *[from time1 to time2]* field. During this update postponement period specified by the *[from time1 to time2]* field, the specified users (which may be all users) can/are authorized to update the data specified in the *<relation> [(field-comma list)]* field, but after the time specified in the *[from time1 to time2]* field the specified users may not update the data *<relation> [(field-comma list)]* field (which may be all data)/data update is prohibited. Note that time1 in the *[from time1 to time2]* field can be specified as the time of insertion for the data.) (Page 691, Under Heading: **Discretionary Access Control**).

As per claim 11, Glover discloses said insert-only attribute being specified to a column of said database (i.e. *"In a database environment, access control must be expanded to arbitrate accesses to a finer detail, such as to the attribute or tuple level."*) The preceding text excerpt clearly indicates that the access control/insert only attribute is specified to the attribute level/to a column of said database. Note that not only is the attribute level synonymous with a column of a database, but also that to implement this a table would need to be created which would hold the access right/insert only attribute information for each column in the database, therefor making the access right/insert only

attribute information specified within a column of a database.) (Page 690, Under Heading: **Need for Database Security and Data Integrity**).

### ***Claim Rejections - 35 USC § 103***

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claim 5 rejected under 35 U.S.C. 103(a) as being unpatentable over Glover et al ("Multilevel Secure Databases: A New Approach", IEEE Proceedings of Southeastcon '91, Apr. 1991; Vol. 2, Pgs 690-694, and referred to hereinafter as Glover) in view of Prakash (U.S. Pre Grant Publication Number 2005/0165868).

As per Claim 5, Glover discloses a database management method, comprising the steps of: entering a database definition request including identification information for specifying a database and access attribute information of said database (i.e. "*The data dictionary contains the database schema and characteristics of data attributes. The data dictionary is invoked for data validation whenever a query is posed or data is updated or added to the database...The data dictionary may also contain information about discretionary access privileges and the location of database files which contain the actual data.*" The preceding text excerpt clearly indicates that whenever a query/update/data addition is requested the data dictionary is invoked and provides information about/defines the database (in affect making the query/update/data addition a data definition request), such information including the database schema/characteristics of data attributes/identification information for specifying a database and information about discretionary access privileges/access

Art Unit: 2165

attribute information of said database.) (Page 692, Under Heading: **Secure Data Dictionary**); if said access attribute information is an insert-only attribute, authorizing data insertion and access to data in said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified with only the insert privilege/is an insert-only attribute, then only access to the data and data insertion will be allowed/authorized.) (Page 691, Under Heading: **Discretionary Access Control**); specifying at least an attribute of data update prohibition to said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing. INGRES controls access to relations using the GRANT statement which is of the form: GRANT <privileges> on <relation> to <user,...> where privileges are select, insert, delete, update."* The preceding text excerpt clearly indicates that if the access rights of the user entering the query/update/data addition/data definition request are specified as not including the update right/specifying an attribute of data update prohibition, the user will not be able to update database information.) (Page 691, Under Heading: **Discretionary Access Control**); disabling change of said attribute after said attribute is specified (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists."* The preceding text excerpt clearly indicates that another user is not able to grant any privileges to a user not granted by the DBA, nor

Art Unit: 2165

is the user able to change the level of their access rights (i.e. change of said attribute is disabled.) (Page 691, Under Heading: **Discretionary Access Control**), and that said database with said insert-only attribute holds an unload date and time in said database (i.e. *"In INGRES, the database administrator (DBA) is responsible for the creation and destruction of all shared relations and also for all authorization. No mechanism for the delegation of this responsibility exists. This means that we do not have to be concerned with propagation of access rights between users since the DBMS allows only one level sharing...Access control rules are written by the DBA using QUEL. Integrity constraints are expressed in QUEL by the DEFINE PERMIT statement as follows: DEFINE PERMIT <operations> on <relation> [(field-comma list)] to user [at terminal] [from time1 to time2] [on day1 to day2] [where condition]"* The preceding text excerpt clearly indicates that using the DEFINE PERMIT statement, a time where date updates and deletions/an unload date and time could be specified by specifying that updates and deletions are allowed in the <operations> field, and specifying that these operations are allowed during the time period specified in the [from time1 to time2] field on the day specified in the [on day1 to day2] field.) (Page 691, Under Heading: **Discretionary Access Control**).

Glover fails to disclose in the case of reloading said database, determined if said unload date and time is matched to that stored in an external storage medium, and if matched, the process of reloading said database is executed.

Prakash discloses in the case of reloading said database, determined if said unload date and time is matched to that stored in an external storage medium (i.e. *"A user can set policies to schedule and manage the restore operations...A Recover Database Utility lets a user restore information from a database backup to the database...including an option to specify a date to restore the database."* The preceding text excerpt clearly indicates that a date/scheduled time/unload date and time is stored along with database data in a database backup/external storage medium and that the dates are managed/matched.) (Page 6, Paragraphs 64, 72), and if matched, the process of reloading said database is executed (i.e. *"...the database session created on or before this date*

Art Unit: 2165

*will be used for backup.*" The preceding text excerpt clearly indicates that if the date of the database session is matched to the specified date, that that session will be used as the backup of the database in the restore operation.) (Page 6, Paragraphs 72).

It would be obvious to one skilled in the art at the time of Applicants invention to modify the teachings of Glover with the teachings of Prakash to include, in the case of reloading said database, determining if said unload date and time is matched to that stored in an external storage medium, and if matched, the process of reloading said database is executed with the motivation to specify a date to restore the database (Prakash, Page 6, Paragraph 72).




***Points Of Contact***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Hicks whose telephone number is (571) 272-2670. The examiner can normally be reached on Monday - Friday 8:30a - 5:00p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Gaffin can be reached on (571) 272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Michael J Hicks  
Technology Center 2100  
Art Unit 2165  
(571) 272-2670

  
JEFFREY GAFFIN  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100